

日本特許庁  
JAPAN PATENT OFFICE

CFO 15945 VS/hda  
09/987, 832  
SHIRO WAKAO, et al  
11/16/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年11月12日

出願番号

Application Number:

特願2001-346689

出願人

Applicant(s):

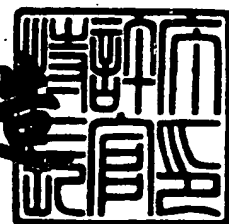
キヤノン株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年12月14日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3108563

【書類名】 特許願

【整理番号】 4516095

【提出日】 平成13年11月12日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 5/00

【発明の名称】 画像検証システム、画像検証装置、画像検証方法、プログラム及び記録媒体

【請求項の数】 37

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社  
社内

    【氏名】 若尾 聡

【発明者】

    【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社  
社内

    【氏名】 岩村 恵市

【特許出願人】

    【識別番号】 000001007

    【氏名又は名称】 キヤノン株式会社

【代理人】

    【識別番号】 100090273

    【弁理士】

    【氏名又は名称】 國分 孝悦

    【電話番号】 03-3590-8901

【先の出願に基づく優先権主張】

    【出願番号】 特願2000-351529

    【出願日】 平成12年11月17日

【手数料の表示】

    【予納台帳番号】 035493

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705348

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像検証システム、画像検証装置、画像検証方法、プログラム及び記録媒体

【特許請求の範囲】

【請求項 1】 画像生成装置と、第 1 の画像検証装置とを備えた画像検証システムであって、

前記画像生成装置は、

画像データを生成する画像データ生成手段と、

前記画像データと、第 1 の情報とを用いて前記画像データの第 1 の検証データを生成する第 1 の検証データ生成手段とを備え、

前記第 1 の画像検証装置は、

前記画像データと、前記第 1 の検証データと、前記第 1 の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、

前記画像データが改変されていない場合、前記画像データと、第 2 の情報とを用いて前記画像データの第 2 の検証データを生成する第 2 の検証データ生成手段とを備えることを特徴とする画像検証システム。

【請求項 2】 前記第 1 の検証データ生成手段は、ハッシュ関数と所定の演算とを用いて前記第 1 の検証データを生成することを特徴とする請求項 1 に記載の画像検証システム。

【請求項 3】 前記第 2 の検証データ生成手段は、ハッシュ関数と公開鍵暗号とを用いて前記第 2 の検証データを生成することを特徴とする請求項 1 または 2 に記載の画像検証システム。

【請求項 4】 前記第 2 の検証データ生成手段は、前記画像データが改変されている場合、前記第 2 の検証データの生成を禁止することを特徴とする請求項 1 ～ 3 の何れか 1 項に記載の画像検証システム。

【請求項 5】 前記第 1 の画像検証装置は、前記第 1 の情報と前記第 2 の情報との対応関係を記憶したメモリを備えることを特徴とする請求項 1 ～ 4 の何れか 1 項に記載の画像検証システム。

【請求項 6】 前記第 1 の情報は、前記画像生成装置を特定する ID 情報で

あることを特徴とする請求項 1 ～ 5 の何れか 1 項に記載の画像検証システム。

【請求項 7】 前記第 2 の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項 1 ～ 6 の何れか 1 項に記載の画像検証システム。

【請求項 8】 前記画像検証システムは更に、第 2 の画像検証装置を備え、前記第 2 の画像検証装置は、前記画像データと、前記第 2 の検証データと、前記第 2 の情報に対応する第 3 の情報とを用いて前記画像データが改変されているか否かを検証する検証手段を備えることを特徴とする請求項 1 ～ 7 の何れか 1 項に記載の画像検証システム。

【請求項 9】 前記第 2 の情報は、公開鍵暗号方式の秘密鍵であり、前記第 3 の情報は、公開鍵暗号方式の公開鍵であることを特徴とする請求項 8 に記載の画像検証システム。

【請求項 1 0】 前記第 2 の画像検証装置は、前記第 1 の画像検証装置をクライアントとするサーバコンピュータであることを特徴とする請求項 8 または 9 に記載の画像検証システム。

【請求項 1 1】 前記画像生成装置は、撮像部を備えた電子機器であることを特徴とする請求項 1 ～ 1 0 の何れか 1 項に記載の画像検証システム。

【請求項 1 2】 前記画像生成装置は、デジタルカメラ、カメラ一体型デジタルカメラまたはスキャナであることを特徴とする請求項 1 1 に記載の画像検証システム。

【請求項 1 3】 画像生成装置と、第 1 の装置と、第 2 の装置を備えた画像検証システムであって、

前記画像生成装置は、

画像データを生成する画像データ生成手段と、

前記画像データと、第 1 の情報とを用いて前記画像データの第 1 の検証データを生成する第 1 の検証データ生成手段とを備え、

前記第 1 の装置は、

前記画像データと、前記第 1 の検証データとを前記第 2 の装置に送信する送信手段を備え、

前記第 2 の装置は、

前記画像データと、前記第 1 の検証データと、前記第 1 の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、

前記画像データが改変されていない場合、前記画像データと、第 2 の情報とを用いて前記画像データの第 2 の検証データを生成する第 2 の検証データ生成手段とを備えることを特徴とする画像検証システム。

【請求項 1 4】 前記第 1 の検証データ生成手段は、ハッシュ関数と、所定の演算とを用いて前記第 1 の検証データを生成することを特徴とする請求項 1 3 に記載の画像検証システム。

【請求項 1 5】 前記第 2 の検証データ生成手段は、ハッシュ関数と、公開鍵暗号とを用いて前記第 2 の検証データを生成することを特徴とする請求項 1 3 または 1 4 に記載の画像検証システム。

【請求項 1 6】 前記第 2 の検証データ生成手段は、前記画像データが改変されている場合、前記第 2 の検証データの生成を禁止することを特徴とする請求項 1 3 ～ 1 5 の何れか 1 項に記載の画像検証システム。

【請求項 1 7】 前記第 2 の装置は、前記第 1 の情報と前記第 2 の情報との対応関係を記憶したメモリを備えることを特徴とする請求項 1 3 ～ 1 6 の何れか 1 項に記載の画像検証システム。

【請求項 1 8】 前記第 1 の情報は、前記画像生成装置を特定する ID 情報であることを特徴とする請求項 1 3 ～ 1 7 の何れか 1 項に記載の画像検証システム。

【請求項 1 9】 前記第 2 の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項 1 3 ～ 1 8 の何れか 1 項に記載の画像検証システム。

【請求項 2 0】 前記第 2 の装置は、IC カードまたはマイクロプロセッサ付き記憶媒体であることを特徴とする請求項 1 3 ～ 1 9 の何れか 1 項に記載の画像検証システム。

【請求項 2 1】 前記第 2 の装置は、前記第 1 の装置をクライアントとするサーバコンピュータであることを特徴とする請求項 1 3 ～ 1 9 の何れか 1 項に記載の画像検証システム。

【請求項 2 2】 前記画像検証システムは更に、画像検証装置を備え、前記

画像検証装置は、前記画像データと、前記第 2 の検証データと、前記第 2 の情報に対応する第 3 の情報とを用いて前記画像データが改変されているか否かを検証する検証手段を備えることを特徴とする請求項 1 3 ～ 2 1 の何れか 1 項に記載の画像検証システム。

【請求項 2 3】 前記第 2 の情報は、公開鍵暗号方式の秘密鍵であり、前記第 3 の情報は、公開鍵暗号方式の公開鍵であることを特徴とする請求項 2 2 に記載の画像検証システム。

【請求項 2 4】 前記画像検証装置は、前記第 1 の装置をクライアントとするサーバコンピュータであることを特徴とする請求項 2 2 または 2 3 に記載の画像検証システム。

【請求項 2 5】 前記画像生成装置は、撮像部を備えた電子機器であることを特徴とする請求項 1 3 ～ 2 4 の何れか 1 項に記載の画像検証システム。

【請求項 2 6】 前記画像生成装置は、デジタルカメラ、カメラ一体型デジタルカメラまたはスキャナであることを特徴とする請求項 2 5 に記載の画像検証システム。

【請求項 2 7】 画像データと、前記画像データの第 1 の検証データと、第 1 の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、

前記画像データが改変されていない場合、前記画像データと、第 2 の情報とを用いて前記画像データの第 2 の検証データを生成する生成手段とを備えることを特徴とする画像検証装置。

【請求項 2 8】 前記生成手段は、ハッシュ関数と公開鍵暗号とを用いて前記第 2 の検証データを生成することを特徴とする請求項 2 7 に記載の画像検証装置。

【請求項 2 9】 前記第 2 の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項 2 7 または 2 8 に記載の画像検証装置。

【請求項 3 0】 前記生成手段は、前記画像データが改変されている場合、前記第 2 の検証データの生成を禁止することを特徴とする請求項 2 7 ～ 2 9 の何れか 1 項に記載の画像検証装置。

【請求項 3 1】 前記画像検証装置は、前記第 1 の情報と前記第 2 の情報との対応関係を記憶したメモリを備えることを特徴とする請求項 2 7 ～ 3 0 の何れか 1 項に記載の画像検証装置。

【請求項 3 2】 画像データと、前記画像データの第 1 の検証データと、第 1 の情報とを用いて前記画像データが改変されているか否かを検証する検証ステップと、

前記画像データが改変されていない場合、前記画像データと、第 2 の情報とを用いて前記画像データの第 2 の検証データを生成する生成ステップとを有することを特徴とする画像検証方法。

【請求項 3 3】 前記検証データ生成ステップは、ハッシュ関数と公開鍵暗号とを用いて前記第 2 の検証データを生成することを特徴とする請求項 3 2 に記載の画像検証方法。

【請求項 3 4】 前記第 2 の情報は、公開鍵暗号方式の秘密鍵であることを特徴とする請求項 3 2 または 3 3 に記載の画像検証方法。

【請求項 3 5】 前記生成ステップは、前記画像データが改変されている場合、前記第 2 の検証データの生成を禁止することを特徴とする請求項 3 2 ～ 3 4 の何れか 1 項に記載の画像検証方法。

【請求項 3 6】 請求項 3 2 ～ 3 5 の何れか 1 項に記載の画像検証方法をコンピュータに実行させるためのプログラム。

【請求項 3 7】 請求項 3 6 に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタルカメラなどの画像生成装置で生成された画像データの改変を検出する画像検証システム、画像生成装置、画像生成方法、プログラム及び記録媒体に関するものである。

【0 0 0 2】

【従来技術】



近年、被写体の光学像をデジタル化して記憶するデジタルカメラが実用化されている。

デジタルカメラで撮影された画像データは、パーソナルコンピュータに取り込むことが簡単にできる反面、パーソナルコンピュータ上で簡単に改変することができるという問題があった。そのため、デジタルカメラで撮影された画像データの信頼性は、銀塩写真よりも低く、証拠能力が乏しいという問題があった。そこで、近年、デジタルカメラで撮影された画像データにデジタル署名を付加する機能を備えたデジタルカメラシステムが提案されている。従来のデジタル署名機能付きデジタルカメラシステムは、例えば、米国特許第 5, 4 9 9, 2 9 4、特開平 9 - 2 0 0 7 3 0 号などに開示されている。

#### 【0003】

##### 【発明が解決しようとする課題】

デジタル署名の生成には、通常、RSA暗号などの公開鍵暗号方式が利用される。しかしながら、RSA暗号などの公開鍵暗号方式は、べき乗演算や剰余演算が必要であるために高速な処理が難しく、DESなどの共通鍵暗号方式に比べて数百倍から数千倍の処理時間が必要である。そのため、従来のデジタルカメラの限られた演算リソースでは、デジタル署名の生成が大変難しいという問題があった。デジタルカメラの演算リソースの性能を大幅に向上させ、デジタル署名の生成を容易に行えるようにする方法もあるが、このような方法ではデジタルカメラ本体にかかるコストが非常に増大してしまうため好ましくない。

#### 【0004】

本発明は、上述の問題点に鑑みてなされたものであり、デジタルカメラなどの画像生成装置にかかるコストの増大を防ぎつつ、画像生成装置で撮影された画像データが改変されているか否かを確実に検出することのできる画像検証システム、画像検証装置、画像検証方法、プログラム及び記録媒体を提供することを目的とする。

#### 【0005】

##### 【課題を解決するための手段】

本発明の画像検証システムは、画像生成装置と、第1の画像検証装置とを備え

た画像検証システムであって、前記画像生成装置は、画像データを生成する画像データ生成手段と、前記画像データと、第1の情報とを用いて前記画像データの第1の検証データを生成する第1の検証データ生成手段とを備え、前記第1の画像検証装置は、前記画像データと、前記第1の検証データと、前記第1の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、前記画像データが改変されていない場合、前記画像データと、第2の情報とを用いて前記画像データの第2の検証データを生成する第2の検証データ生成手段とを備えることを特徴とする。

## 【0006】

また、本発明の画像検証システムは、画像生成装置と、第1の装置と、第2の装置を備えた画像検証システムであって、前記画像生成装置は、画像データを生成する画像データ生成手段と、前記画像データと、第1の情報とを用いて前記画像データの第1の検証データを生成する第1の検証データ生成手段とを備え、前記第1の装置は、前記画像データと、前記第1の検証データとを前記第2の装置に送信する送信手段を備え、前記第2の装置は、前記画像データと、前記第1の検証データと、前記第1の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、前記画像データが改変されていない場合、前記画像データと第2の情報とを用いて前記画像データの第2の検証データを生成する第2の検証データ生成手段とを備えることを特徴とする。

## 【0007】

また、本発明の画像検証装置は、画像データと、前記画像データの第1の検証データと、第1の情報とを用いて前記画像データが改変されているか否かを検証する検証手段と、前記画像データが改変されていない場合、前記画像データと、第2の情報とを用いて前記画像データの第2の検証データを生成する生成手段とを備えることを特徴とする。

## 【0008】

また、本発明の画像検証方法は、画像データと、前記画像データの第1の検証データと、第1の情報とを用いて前記画像データが改変されているか否かを検証する検証ステップと、前記画像データが改変されていない場合、前記画像データ

と、第 2 の情報とを用いて前記画像データの第 2 の検証データを生成する生成ステップとを有することを特徴とする。

【 0 0 0 9 】

【発明の実施の形態】

（第 1 の実施の形態）

以下、図面を参照し、本発明に好適な第 1 の実施の形態について説明する。

まず、図 1 2 を参照し、第 1 の実施の形態における画像データ検証システムの構成の一例を説明する。

【 0 0 1 0 】

1 0 は、被写体の画像データと、その画像データの完全性を検証するための 1 次検証データとを生成し、1 次検証データ付き画像ファイルを生成する画像生成装置である。なお、画像生成装置 1 0 は、デジタルカメラ、カメラ一体型デジタルビデオレコーダ、スキャナなどの撮像装置であっても、被写体の画像データを撮影する機能を備えた電子機器であってもよい。

【 0 0 1 1 】

2 0 は、1 次検証データ付き画像ファイル内の画像データの完全性を検証し、その画像データが改変されているか否かを検出する検証データ変換装置である。また、検証データ変換装置 2 0 は、その画像データの完全性が確認された場合（即ち、その画像データが改変されていない場合）、その画像データの完全性及び正当性を検証するための 2 次検証データ（即ち、デジタル署名）を生成し、1 次検証データ付き画像ファイルを 2 次検証データ付き画像ファイルに変換する。なお、検証データ変換装置 2 0 は、パーソナルコンピュータなどのコンピュータである。

【 0 0 1 2 】

3 0 は、2 次検証データ付き画像ファイル内の画像データの完全性を検証し、その画像データが改変されているか否かを検出する画像検証装置である。なお、画像検証装置 3 0 は、パーソナルコンピュータなどのコンピュータであっても、検証データ変換装置 2 0 をクライアントとするサーバコンピュータであってもよい。

## 【 0 0 1 3 】

画像生成装置 1 0 と検証データ変換装置 2 0 との間は、LAN、IEEE 1 3 9 4 - 1 9 9 5、USB (Universal Serial Bus) などのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。また、検証データ変換装置 2 0 と画像検証装置 3 0 との間を接続する媒体は、LAN、WAN、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。

## 【 0 0 1 4 】

次に、第 1 の実施の形態における画像生成装置 1 0 の構成について説明する。図 1 は、第 1 の実施の形態における画像生成装置 1 0 の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

## 【 0 0 1 5 】

1 1 は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。1 4 は、CCD（電荷結合素子）などの光学センサーを含む撮像部である。1 5 は、1 次検証データ付き画像ファイルを記憶する保管用メモリである。1 6 は、1 次検証データ付き画像ファイルを検証データ変換装置 2 0 に送信するインターフェース部である。1 7 は、プログラムメモリである。プログラムメモリ 1 7 は、1 次検証データ付き画像ファイルを生成する機能を制御するプログラムを記憶している。また、プログラムメモリ 1 7 は、1 次検証データの生成に必要な共通情報 K c（これは、共通鍵暗号方式の暗号鍵に相当する）と、画像生成装置 1 0 の固有 ID（画像生成装置 1 0 だけを特定可能な識別子であればよい。例えば、製造番号、シリアル番号など）とを記憶している。なお、プログラムメモリ 1 7 は、ROMであっても、EEPROMであってもよい。但し、プログラムメモリ 1 7 内の情報は、外部に漏れないように秘密に管理するものとする。1 8 は、ユーザからの様々な指示（撮影の開始など）を受け付ける操作部である。

## 【 0 0 1 6 】

次に、第 1 の実施の形態における検証データ変換装置 2 0 の構成について説明

する。図 2 は、第 1 の実施の形態における検証データ変換装置 2 0 の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

#### 【0017】

2 1 は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。2 4 は、画像生成装置 1 0 からの 1 次検証データ付き画像ファイルを受信するインターフェース部 A である。2 8 は、画像検証装置 3 0 に 2 次検証データ付き画像ファイルを送信するインターフェース部 B である。2 5 は、1 次検証データ付き画像ファイル及び 2 次検証データ付き画像ファイルを記憶する保管用メモリである。2 6 は、プログラムメモリである。プログラムメモリ 2 6 は、1 次検証データ付き画像ファイルの完全性を検証する機能と、2 次検証データ付き画像ファイルを生成する機能とを制御するプログラムを記憶している。また、プログラムメモリ 2 6 は、複数の画像生成装置の固有 ID と、各固有 ID に対応する共通情報 K c（これは、共通鍵暗号方式の復号鍵に相当する）と、各固有 ID に対応する秘密情報 K s（これは、公開鍵暗号方式の秘密鍵に相当する）とを登録したテーブル T 1 を記憶している。テーブル T 1 の一例を図 7（a）に示す。なお、プログラムメモリ 2 6 は、ROM であっても、EEPROM であってもよい。但し、プログラムメモリ 2 6 内の情報は、外部に漏れないように秘密に管理するものとする。2 7 は、ユーザからの様々な指示を受け付ける操作部である。2 2 は、2 次検証データ付き画像ファイルの画像データが改変されているか否かを示すメッセージをディスプレイ装置、プリンタなどの外部装置に出力する出力部である。

#### 【0018】

次に、第 1 の実施の形態における画像検証装置 3 0 の構成について説明する。図 3 は、第 1 の実施の形態における画像検証装置 3 0 の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

#### 【0019】

3 1 は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である

。34は、2次検証データ付き画像ファイルを受信したり、2次検証データ付き画像ファイルの完全性を検証するときに必要な公開情報Kpを受信したりするインターフェース部である。36は、プログラムメモリである。プログラムメモリ36は、2次検証データ付き画像ファイルの完全性を検証する機能を制御するプログラムを記憶している。また、プログラムメモリ36は、複数の画像生成装置の固有IDと、各固有IDに対応する公開情報Kp（これは、公開鍵暗号方式の公開鍵に相当する）とを登録したテーブルT2を記憶している。テーブルT2の一例を図7（b）に示す。なお、プログラムメモリ36は、ROMであっても、EEPROMであってもよい。37は、ユーザからの様々な指示を受け付ける操作部である。32は、2次検証データ付き画像ファイルに改変があるか否かを示すメッセージをディスプレイ装置、プリンタなどの外部装置に出力する出力部である。35は、2次検証データ付き画像ファイルを記憶する保管用メモリである。また、保管用メモリ35は、改変の有無、登録日時、検証日時などの情報を登録するデータベースを有する。

#### 【0020】

次に、第1の実施の形態における画像データ検証システムの処理手順について説明する。図4は、第1の実施の形態における画像データ検証システムの処理手順について説明する図である。

#### 【0021】

ステップS401：画像生成装置10は、ユーザの撮影指示に従って被写体の画像データを生成し、生成された画像データを所定の画像ファイルフォーマットに準拠した画像ファイルにファイル化する。このとき、画像データは、所定の画像ファイルフォーマットに準拠した画像圧縮符号化方式に従って圧縮符号化される。なお、所定の画像ファイルフォーマットは、JFIF（JPEG File Interchange Format）、TIFF（Tagged Image File Format）及びGIF（Graphics Interchange Format）の何れかであっても、それらを拡張したものであっても、他の画像ファイルフォーマットであってもよい。

#### 【0022】

ステップS402：画像生成装置10は、生成された画像データと共有情報K

c とからその画像データの 1 次検証データを生成する。

【 0 0 2 3 】

図 5 ( a ) 及び図 5 ( b ) を参照し、 1 次検証データの生成方法の一例を説明する。なお、 1 次検証データの生成方法は、 1 次検証データの安全のために、一般には公開されないものであり、画像生成装置 1 0 の内部及び検証データ変換装置 2 0 の内部で秘密に管理されるものである。

【 0 0 2 4 】

図 5 ( a ) は、 1 次検証データの第 1 の生成方法について説明する図である。図 5 ( a ) に示す第 1 の生成方法は、以下の ( a 1 ) ～ ( a 3 ) に示す手順に従って実行される。なお、図 5 ( a ) に示す生成方法は、画像生成装置 1 0 の制御／演算部 1 1 及び検証データ変換装置 2 0 の制御／演算部 2 1 で実行される。

【 0 0 2 5 】

( a 1 ) まず、簡易な演算を実行し、画像データを共有情報 K c で暗号化する。簡易な演算の一例を図 6 に示す。第 1 の実施の形態では、図 6 に示すように、画像データの一部（例えば、最上位バイト）と共有情報 K c （例えば、「 1 1 1 1 1 1 1 1 」）との間で排他的論理和演算を行い、画像データを暗号化する。なお、簡易な演算は、画像生成装置 1 0 の限られた演算リソース上で高速に実行できるものであれば、他の演算アルゴリズムに置き換えてもよい。

【 0 0 2 6 】

( a 2 ) 次に、 ( a 1 ) で得られたデータをハッシュ関数 H 1 によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数 H 1 は、 MD - 2 、 MD - 4 、 MD - 5 、 SHA - 1 、 RIPEMD - 1 2 8 及び RIPEMD - 1 6 0 の何れかであっても、他のハッシュ関数であってもよい。

【 0 0 2 7 】

( a 3 ) 最後に、 ( a 2 ) で得られたダイジェストデータを 1 次検証データとする。

【 0 0 2 8 】

図 5 ( b ) は、 1 次検証データの第 2 の生成方法について説明する図である。図 5 ( b ) に示す生成方法は、以下の ( b 1 ) ～ ( b 3 ) に示す手順に従って実

行される。なお、図 5 (b) に示す第 2 の生成方法は、画像生成装置 1 0 の制御／演算部 1 1 及び検証データ変換装置 2 0 の制御／演算部 2 1 で実行される。

## 【 0 0 2 9 】

(b 1) まず、画像データをハッシュ関数 H 1 によってダイジェストデータ (ハッシュ値) に変換する。なお、ハッシュ関数 H 1 は、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128 及び RIPEMD-160 の何れかであっても、他のハッシュ関数であってもよい。

## 【 0 0 3 0 】

(b 2) 次に、所定の共通鍵暗号方式に従ってダイジェストデータを共有情報 K c で暗号化する。なお、所定の共通鍵暗号方式は、DES または Rijndael であっても、他の共通鍵暗号方式であってもよい。

## 【 0 0 3 1 】

(b 3) 最後に、共有情報 K c で暗号化されたダイジェストデータを 1 次検証データとする。

## 【 0 0 3 2 】

ステップ S 4 0 3 : 画像生成装置 1 0 は、生成された 1 次検証データを画像ファイルのヘッダ部に付加し、1 次検証データ付き画像ファイルを生成する。また、画像生成装置 1 0 は、1 次検証データだけでなく、画像生成装置 1 0 の固有 ID も画像ファイルのヘッダ部に付加する。

## 【 0 0 3 3 】

ステップ S 4 0 4 : 画像生成装置 1 0 は、1 次検証データ付き画像ファイルを検証データ変換装置 2 0 に送信する。

## 【 0 0 3 4 】

ステップ S 4 0 5 : 1 次検証データ付き画像ファイルを受信した後、検証データ変換装置 2 0 は、そのファイルのヘッダ部から 1 次検証データ及び画像生成装置 1 0 の固有 ID を抽出し、そのファイルのデータ部から画像データを抽出する。また、検証データ変換装置 2 0 は、プログラムメモリ 2 6 内のテーブル T 1 を参照し、抽出された固有 ID に対応する共有情報 K c 及び秘密情報 K s を検出する。例えば、画像生成装置 1 0 の固有 ID が「0 0 1」である場合、その固有 ID



Dに対応する共有情報K<sub>c</sub>は「0x1111」であり、その固有IDに対応する秘密情報K<sub>s</sub>は「0x2222」である。検証データ変換装置20は、抽出された画像データと検出された共有情報K<sub>c</sub>とからその画像データの1次検証データを生成する。なお、検証データ変換装置20は、画像生成装置10と同じ生成方法に従って1次検証データを生成する。

## 【0035】

ステップS406：検証データ変換装置20は、1次検証データ付き画像ファイルから抽出された1次検証データ（即ち、画像生成装置10の内部で生成された1次検証データ）と、ステップS405で生成された1次検証データ（即ち、検証データ変換装置20の内部で生成された1次検証データ）とを比較し、1次検証データ付き映像ファイル内の画像データの完全性を検証する。画像生成装置10から検証データ変換装置20に至るまでに改変がなかった場合、2つの1次検証データは一致する。この場合、検証データ変換装置20は、この画像データが画像生成装置10で生成された画像データであり、改竄のない安全な画像データであることを確実に確認することができる。更にこの場合、検証データ変換装置20は、改変なしと判定し、この画像データの2次検証データの生成を開始する。一方、画像生成装置10から検証データ変換装置20に至るまでに改変があった場合、2つの1次検証データは一致しない。この場合、検証データ変換装置20は、改変ありと判定し、この画像データが改変されていることを示すメッセージをユーザに通知する。なお、この場合、検証データ変換装置20は、この画像データの2次検証データの生成を禁止する。

## 【0036】

ステップS407：改変なしと判定した場合、検証データ変換装置20は、1次検証データ付き画像ファイル内の画像データから2次検証データ（即ち、デジタル署名）を生成する。

## 【0037】

図8を参照し、2次検証データの生成方法を説明する。図8に示す生成方法は、以下の（1）～（3）に示す手順に従って実行される。なお、図8に示す生成方法は、検証データ変換装置20の制御／演算部21及び画像検証装置30の制

御／演算部 31 で実行される。

【0038】

(1) まず、画像データをハッシュ関数 H2 によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数 H2 は、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128 及び RIPEMD-160 の何れかであっても、他のハッシュ関数であってもよい。

【0039】

(2) 次に、所定の公開鍵暗号方式に従ってダイジェストデータを秘密情報 K<sub>s</sub> で暗号化する。なお、所定の公開鍵暗号方式は、RSA 暗号方式であっても、他の公開鍵暗号方式であってもよい。

【0040】

(3) 最後に、秘密情報 K<sub>s</sub> で暗号化されたダイジェストデータを 2 次検証データ（即ち、デジタル署名）とする。

【0041】

ステップ S408：検証データ変換装置 20 は、画像ファイルのヘッダ部にある 1 次検証データを 2 次検証データに置き換え、2 次検証データ付き画像ファイルを生成する。生成された 2 次検証データ付き画像ファイルは、インターネットなどのネットワーク、または、メモ리카ードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力される。画像検証装置 30 は、インターネットなどのネットワーク、または、メモ리카ードなどのリムーバブルメディア（着脱可能な記憶媒体）から 2 次検証データ付き画像ファイルを入力する。

【0042】

ステップ S409：2 次検証データ付き画像ファイルを入力した後、画像検証装置 30 は、そのファイルのヘッダ部から 2 次検証データ及び画像生成装置 10 の固有 ID を抽出する。また、画像検証装置 30 は、プログラムメモリ 36 内のテーブル T2 を参照し、抽出された固有 ID に対応する公開情報 K<sub>p</sub> を検出する。例えば、画像生成装置 10 の固有 ID が「001」の場合、その固有 ID に対応する公開情報 K<sub>p</sub> は「0x3333」である。なお、公開情報 K<sub>p</sub> は、所定のサーバから取得してもよい。画像検証装置 30 は、抽出された 2 次検証データを

検出された公開情報 $K_p$ で復号化し、ダイジェストデータ（ハッシュ値）を復元する。なお、公開情報 $K_p$ は、検証データ変換装置20が秘密に管理している秘密情報 $K_s$ に対応する情報であり、一般に公開されている情報である。

## 【0043】

ステップS410：また、画像検証装置30は、2次検証データ付き画像ファイルのデータ部から画像データを抽出する。画像検証装置30は、抽出された画像データをハッシュ関数 $H_2$ によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数 $H_2$ は、検証データ変換装置20のハッシュ関数 $H_2$ と同じハッシュ関数である。

## 【0044】

ステップS411：画像検証装置30は、ステップS409で復元されたダイジェストデータと、ステップS410で得られたダイジェストデータとを比較し、2次検証データ付き映像ファイル内の画像データの完全性及び正当性を検証する。検証データ変換装置20から画像検証装置30に至るまでに改変がなかった場合、2つのダイジェストデータは一致する。この場合、2次検証装置30は、この画像データが画像生成装置10で生成された画像データであることと、この画像データの2次検証データは1次検証装置20で付加されたものであることを確実に確認することができる。更にこの場合、画像検証装置30は、改変なしと判定し、その判定結果をユーザに通知する。一方、検証データ変換装置20から画像検証装置30に至るまでに改変があった場合、2つのダイジェストデータは一致しない。この場合、画像検証装置30は、改変ありと判定し、その判定結果をユーザに通知する。

## 【0045】

ステップS412：画像検証装置30は、2次検証データ付き画像ファイルの改変をチェックするごとに、画像ファイルのファイル名、画像ファイルの登録日時、画像ファイルの検証日時、改変の有無などの情報を保管用メモリ35のデータベースに登録する。このような情報を保管用メモリに登録することで、検証者は、検証された2次検証データ付き画像ファイルを管理することができる。

## 【0046】

以上説明したように、第1の実施の形態における画像データ検証システムによれば、画像生成装置10の演算リソースの性能を大幅に向上させることなく、画像生成装置10で生成された画像データが改変されているか否かを確実に検出することができる。

## 【0047】

また、第1の実施の形態における画像データ検証システムによれば、画像生成装置10にかかるコストを低減することができる。

また、第1の実施の形態における画像データ検証システムによれば、画像生成装置10の固有IDに対応する共有情報K<sub>c</sub>、秘密情報K<sub>s</sub>及び公開情報K<sub>p</sub>を用いて1次検証データ及び2次検証データを検証することにより、1次検証データ付き画像ファイル内の画像データまたは2次検証データ付き画像ファイル内の画像データが画像生成装置10で生成されたものであるか否かを確実に確認することができる。

## 【0048】

また、第1の実施の形態における画像データ検証システムによれば、画像生成装置10と検証データ変換装置20との間を1次検証データによって安全に保護することができ、検証データ変換装置20と画像検証装置30との間を2次検証データ（即ち、デジタル署名）によって安全に保護することができるので、システム全体の安全に運用することができる。

## 【0049】

次に、図9のフローチャートを参照し、第1の実施の形態における画像生成装置10の処理手順について説明する。なお、図9に示す処理手順は、プログラムメモリ17のプログラムに従って実行される。また、図9に示す処理手順は、1枚の画像データを撮像するごとに実行される。

## 【0050】

ステップS91：撮像部14は、ユーザの指示に従って被写体の画像データを生成する。制御／演算部11は、撮像部14で生成された画像データを所定の画像ファイルフォーマットに準拠した画像ファイルにファイル化する。

## 【0051】

ステップ S 9 2 : 制御／演算部 1 1 は、生成された画像データと共有情報 K c とからその画像データの 1 次検証データを生成する。

## 【 0 0 5 2 】

ステップ S 9 3 : 制御／演算部 1 1 は、生成された 1 次検証データを画像ファイルのヘッダ部に付加し、1 次検証データ付き画像ファイルを生成する。また、制御／演算部 1 1 は、1 次検証データだけでなく、画像生成装置 1 0 の固有 I D 情報（即ち、固有 I D）も画像ファイルのヘッダ部に付加する。

## 【 0 0 5 3 】

ステップ S 9 4 : インターフェース部 1 6 は、1 次検証データ付き画像ファイルを外部に出力する。

## 【 0 0 5 4 】

以上の処理手順により、画像生成装置 1 0 は、1 つの画像データを生成するごとに、その画像データの 1 次検証データを生成し、画像データとその 1 次検証データと画像生成装置 1 0 の固有 I D とを 1 つの画像ファイルにファイル化することができる。

## 【 0 0 5 5 】

次に、図 1 0 のフローチャートを参照し、第 1 の実施の形態における検証データ変換装置 2 0 の処理手順について説明する。なお、図 1 0 に示す処理手順は、プログラムメモリ 2 6 のプログラムに従って実行される。また、図 1 0 に示す処理手順は、1 次検証データ付き画像ファイルを入力するごとに実行される。

## 【 0 0 5 6 】

ステップ S 1 0 1 : インターフェース部 2 4 は、外部から 1 次検証データ付き画像ファイルを入力する。

## 【 0 0 5 7 】

ステップ S 1 0 2 : 制御／演算部 2 1 は、1 次検証データ付き画像ファイルのヘッダ部から 1 次検証データを抽出する。

## 【 0 0 5 8 】

ステップ S 1 0 3 : また、制御／演算部 2 1 は、1 次検証データ付き画像ファイルのヘッダ部から画像生成装置 1 0 の固有 I D を抽出し、そのファイルのデー

タ部から画像データを抽出する。制御／演算部 21 は、プログラムメモリ 26 内のテーブル T1 を参照し、抽出された固有 ID に対応する共有情報 Kc 及び秘密情報 Ks を検出する。制御／演算部 21 は、抽出された画像データと検出された共有情報 Kc とからその画像データの 1 次検証データを生成する。

## 【0059】

ステップ S104：ステップ S102 で抽出された 1 次検証データ（即ち、画像生成装置 10 の内部で生成された 1 次検証データ）と、ステップ S103 で生成された 1 次検証データ（即ち、検証データ変換装置 20 の内部で生成された 1 次検証データ）とを比較し、画像データの完全性を検証する。2 つの 1 次検証データの一致が検出された場合、ステップ S105 に進む。一方、2 つの 1 次検証データの一致が検出されなかった場合、ステップ S106 に進む。

## 【0060】

ステップ S105：この場合、制御／演算部 21 は、改変ありと判定し、画像データが改変されていることを示すメッセージをユーザに通知する。なお、この場合、画像生成装置 10 は、2 次検証データの生成を禁止する。

## 【0061】

ステップ S106：この場合、制御／演算部 21 は、1 次検証データ付き画像ファイル内の画像データから 2 次検証データ（即ち、デジタル署名）を生成する。

## 【0062】

ステップ S107：制御／演算部 21 は、画像ファイルのヘッダ部にある 1 次検証データを生成された 2 次検証データに置き換え、2 次検証データ付き画像ファイルを生成する。生成された 2 次検証データ付き画像ファイルは、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力される。

## 【0063】

以上の処理手順により、検証データ変換装置 20 は、画像生成装置 10 の演算リソースの性能を大幅に向上させることなく、画像生成装置 10 で生成された画像データが改変されているか否かを確実に検出することができる。また、検証デ

ータ変換装置 2 0 は、1 次検証データ付き画像ファイルの画像データが画像生成装置 1 0 で生成されたものであるか否かを確実に確認することができる。また、1 次検証データ付き画像ファイルの完全性が確認できれば、そのファイルを 2 次検証データ付き画像ファイル（即ち、デジタル署名付き画像ファイル）に変換することもできる。

## 【 0 0 6 4 】

次に、図 1 1 のフローチャートを参照し、第 1 の実施の形態における画像検証装置 3 0 の処理手順について説明する。なお、図 1 1 に示す処理手順は、プログラムメモリ 3 6 のプログラムに従って実行される。また、図 1 1 に示す処理手順は、2 次検証データ付き画像ファイルを入力するごとに実行される。

## 【 0 0 6 5 】

ステップ S 1 1 1 : インターフェース部 3 4 は、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）から 2 次検証データ付き画像ファイルを入力する。

## 【 0 0 6 6 】

ステップ S 1 1 2 : 画像検証装置 3 0 は、2 次検証データ付き画像ファイルのヘッダ部から画像生成装置 1 0 の固有 I D を抽出する。また、画像検証装置 3 0 は、プログラムメモリ 3 6 内のテーブル T 2 を参照し、抽出された固有 I D に対応する公開情報 K p を検出する。なお、公開情報 K p は、所定のサーバから取得してもよい。

## 【 0 0 6 7 】

ステップ S 1 1 3 : 制御／演算部 3 1 は、2 次検証データ付き画像ファイルのヘッダ部から 2 次検証データを抽出する。

## 【 0 0 6 8 】

ステップ S 1 1 4 : 制御／演算部 3 1 は、ステップ S 1 1 3 で抽出された 2 次検証データを公開情報 K p で復号化し、ダイジェストデータ（ハッシュ値）を復元する。

## 【 0 0 6 9 】

ステップ S 1 1 5 : 制御／演算部 3 1 は、2 次検証データ付き画像ファイルの

データ部から画像データを抽出し、抽出された画像データをハッシュ関数H2によってダイジェストデータ（ハッシュ値）に変換する。

## 【0070】

ステップS116：制御／演算部31は、ステップS114で復元されたダイジェストデータと、ステップS115で得られたダイジェストデータとを比較し、画像データの完全性及び正当性を検証する。2つのダイジェストデータの一致が検出された場合には、ステップS118に進む。一方、2つのダイジェストデータの一致が検出されなかった場合には、ステップS117に進む。

## 【0071】

ステップS117：この場合、制御／演算部31は、改変ありと判定し、画像データが改変されていることを示すメッセージをユーザに通知する。

## 【0072】

ステップS118：この場合、制御／演算部31は、改変なしと判定し、画像データが改変されていないことを示すメッセージをユーザに通知する。

## 【0073】

ステップS119：制御／演算部31は、画像ファイルのファイル名、画像ファイルの登録日時、画像ファイルの検証日時、改変の有無などの情報を保管用メモリ35のデータベースに登録する。

## 【0074】

以上の処理手順により、画像検証装置30は、画像生成装置10で生成された画像データが改変されているか否かを確実に検出することができる。また、画像検証装置30は、2次検証データ付き画像ファイルの画像データが画像生成装置10で生成されたものであるか否かを確実に確認することができる。

## 【0075】

以上説明したように、第1の実施の形態における画像データ検証システムによれば、画像生成装置10の演算リソースの性能を大幅に向上させることなく、画像生成装置10で生成された画像データが改変されているか否かを確実に検出することができる。

## 【0076】



## (第2の実施の形態)

以下、図面を参照し、本発明に好適な第2の実施の形態について説明する。第2の実施の形態では、第1の実施の形態の検証データ変換装置20を2つのデータ処理装置によって構成し、共有情報K<sub>c</sub>及び秘密情報K<sub>s</sub>の安全性を向上させる場合について説明する。

## 【0077】

まず、図13を参照し、第2の実施の形態における画像データ検証システムの構成の一例を説明する。なお、画像生成装置10及び画像検証装置30の構成及びそれらが実行する処理手順は、第1の実施の形態と同じであるので、第2の実施の形態ではその説明を省略する。

## 【0078】

20Aは、第1の検証データ変換装置である。20Bは、第1の検証データ変換装置20Aよりも外部からの攻撃に強い第2の検証データ変換装置である。検証データ変換装置20Aは、画像生成装置10からの1次検証データ付き画像ファイルを検証データ変換装置20Bに転送し、検証データ変換装置20Bの検証結果をユーザに通知する。検証データ変換装置20Bは、1次検証データ付き画像ファイル内の画像データの完全性を検証し、その画像データが改変されているか否かを検出する。また、検証データ変換装置20Bは、その画像データの完全性が確認された場合（即ち、その画像データが改変されていない場合）、その画像データの完全性及び正当性を検証するための2次検証データ（即ち、デジタル署名）を生成し、1次検証データ付き画像ファイルを2次検証データ付き画像ファイルに変換する。なお、検証データ変換装置20Aは、パーソナルコンピュータなどのコンピュータである。検証データ変換装置20Bは、ICカードなどのマイクロプロセッサ付き記憶媒体であっても、検証データ変換装置20Aをクライアントとするサーバコンピュータであってもよい。検証データ変換装置20Aがクライアントで、検証データ変換装置20Bがサーバである場合、これらの装置の間の接続は、LAN、WAN、インターネットなどのネットワークであればよい。

## 【0079】

画像生成装置 1 0 と検証データ変換装置 2 0 A との間は、LAN、IEEE 1394-1995、USB (Universal Serial Bus) などの伝送媒体、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。また、検証データ変換装置 2 0 A と画像検証装置 3 0 との間は、インターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）を介して接続できればよい。

## 【 0 0 8 0 】

次に、第 2 の実施の形態における検証データ変換装置 2 0 A の構成について説明する。図 1 4 は、第 2 の実施の形態における検証データ変換装置 2 0 A の主要な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

## 【 0 0 8 1 】

1 4 2 1 は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。1 4 2 3 は、画像生成装置 1 0 からの 1 次検証データ付き画像ファイルを受信するインターフェース部 A である。1 4 2 4 は、検証データ変換装置 2 0 A に 1 次検証データ付き画像ファイルを送信したり、検証データ変換装置 2 0 A からの 2 次検証データ付き画像ファイルを受信したりするインターフェース部 B である。1 4 2 8 は、画像検証装置 3 0 に 2 次検証データ付き画像ファイルを送信するインターフェース部 C である。1 4 2 5 は、1 次検証データ付き画像ファイル及び 2 次検証データ付き画像ファイルを記憶する保管用メモリである。1 4 2 6 は、プログラムメモリである。プログラムメモリ 1 4 2 6 は、1 次検証データ付き画像ファイルの完全性を検証する機能を制御するプログラムを記憶している。なお、プログラムメモリ 1 4 2 6 は、ROM であっても、EEPROM であってもよい。1 4 2 7 は、ユーザからの様々な指示を受け付ける操作部である。1 4 2 2 は、2 次検証データ付き画像ファイルに改変があるか否かを示すメッセージをディスプレイ装置、プリンタなどの外部装置に出力する出力部である。

## 【 0 0 8 2 】

次に、第 2 の実施の形態における検証データ変換装置 2 0 B の構成について説明する。図 1 5 は、第 2 の実施の形態における第 2 の検証データ変換装置の主要

な構成について説明するブロック図である。同図において、各ブロックは機能ごとに分けられた構成要素である。

#### 【0083】

1521は、作業用メモリとマイクロコンピュータとを備えた制御／演算部である。1524は、検証データ変換装置20Aからの1次検証データ付き画像ファイルを受信したり、検証データ変換装置20Aに2次検証データ付き画像ファイルを送信したりするインターフェース部である。1525は、1次検証データ付き画像ファイル及び2次検証データ付き画像ファイルを記憶する保管用メモリである。1526は、プログラムメモリである。プログラムメモリ1526は、2次検証データ付き画像ファイルを生成する機能を制御するプログラムを記憶している。また、プログラムメモリ1526は、複数の画像生成装置の固有IDと、各固有IDに対応する共通情報Kc（これは、共通鍵暗号方式の復号鍵に相当する）と、各固有IDに対応する秘密情報Ks（これは、公開鍵暗号方式の秘密鍵に相当する）とを登録したテーブルT1を記憶している。テーブルT1の一例を図7（a）に示す。なお、プログラムメモリ1526は、ROMであっても、EEPROMであってもよい。但し、プログラムメモリ1526内の情報は、外部に漏れないように秘密に管理するものとする。

#### 【0084】

次に、第2の実施の形態における画像データ検証システムの処理手順について説明する。図16は、第2の実施の形態における画像データ検証システムの処理手順について説明する図である。

#### 【0085】

ステップS1601からステップS1603までの処理手順は、第1の実施の形態のステップS401からステップS403までの処理手順と同様の処理手順であるので、その説明を省略する。

#### 【0086】

ステップS1604：画像生成装置10は、1次検証データ付き画像ファイルを検証データ変換装置20Aに送信する。

#### 【0087】

ステップ S 1 6 0 5 : 検証データ変換装置 2 0 A は、1 次検証データ付き画像ファイルを検証データ変換装置 2 0 B に送信する。

【 0 0 8 8 】

ステップ S 1 6 0 6 : 1 次検証データ付き画像ファイルを受信した後、検証データ変換装置 2 0 B は、そのファイルのヘッダ部から 1 次検証データ及び画像生成装置 1 0 の固有 I D を抽出し、そのファイルのデータ部から画像データを抽出する。また、検証データ変換装置 2 0 B は、プログラムメモリ 1 5 2 6 内のテーブル T 1 を参照し、抽出された固有 I D に対応する共有情報 K c 及び秘密情報 K s を検出する。例えば、固有 I D が「 0 0 1 」の場合、その固有 I D に対応する共有情報 K c は「 0 x 1 1 1 1 」であり、その固有 I D に対応する秘密情報 K s は「 0 x 2 2 2 2 」である。検証データ変換装置 2 0 B は、抽出された画像データと検出された共有情報 K c とからその画像データの 1 次検証データを生成する。なお、検証データ変換装置 2 0 B は、画像生成装置 1 0 と同じ生成方法に従って 1 次検証データを生成する。

【 0 0 8 9 】

ステップ S 1 6 0 7 : 検証データ変換装置 2 0 B は、1 次検証データ付き画像ファイルから抽出された 1 次検証データ（即ち、画像生成装置 1 0 の内部で生成された 1 次検証データ）と、ステップ S 1 6 0 6 で生成された 1 次検証データ（即ち、検証データ変換装置 2 0 B の内部で生成された 1 次検証データ）とを比較し、1 次検証データ付き画像ファイル内の画像データの完全性を検証する。画像生成装置 1 0 から検証データ変換装置 2 0 B に至るまでに改変がなかった場合、2 つの 1 次検証データは一致し、画像データの完全性が確認される。また、同時に、検証データ変換装置 2 0 B は、この画像データが画像生成装置 1 0 で生成された画像データであることを確実に確認することができる。この場合、検証データ変換装置 2 0 B は、改変なしと判定し、画像データの 2 次検証データの生成を開始する。一方、画像生成装置 1 0 から検証データ変換装置 2 0 B に至るまでに改変があった場合、2 つの 1 次検証データは一致せず、画像データの完全性は確認できない。この場合、検証データ変換装置 2 0 B は、改変ありと判定し、画像データが改変されていることを示すメッセージを検証データ変換装置 2 0 A に送

信する。なお、この場合、検証データ変換装置 2 0 B は、画像データの 2 次検証データの生成を禁止する。

【 0 0 9 0 】

ステップ S 1 6 0 8 : 改変なしと判定した場合、検証データ変換装置 2 0 B は、1 次検証データ付き画像ファイルの画像データから 2 次検証データ（即ち、デジタル署名）を生成する。なお、検証データ変換装置 2 0 B は、図 8 に示す生成方法に従って、画像データから 2 次検証データを生成する。

【 0 0 9 1 】

ステップ S 1 6 0 9 : 検証データ変換装置 2 0 B は、画像ファイルのヘッダ部にある 1 次検証データを生成された 2 次検証データに置き換え、2 次検証データ付き画像ファイルを生成する。生成された 2 次検証データ付き画像ファイルは、検証データ変換装置 2 0 A に送信される。

【 0 0 9 2 】

ステップ S 1 6 1 0 : 検証データ変換装置 2 0 A は、2 次検証データ付き画像ファイルをインターネットなどのネットワーク、または、メモ리카ードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力する。

【 0 0 9 3 】

ステップ S 1 6 1 1 : 画像検証装置 3 0 は、インターネットなどのネットワーク、または、メモ리카ードなどのリムーバブルメディア（着脱可能な記憶媒体）から 2 次検証データ付き画像ファイルを入力する。2 次検証データ付き画像ファイルを入力した後、画像検証装置 3 0 は、そのファイルのヘッダ部から 2 次検証データ及び画像生成装置 1 0 の固有 I D を抽出する。また、画像検証装置 3 0 は、プログラムメモリ 3 6 内のテーブル T 2 を参照し、抽出された固有 I D に対応する公開情報 K p を検出する。例えば、固有 I D が「0 0 1」の場合、その固有 I D に対応する公開情報 K p は「0 x 1 1 1 1」であり、その固有 I D に対応する秘密情報 K s は「0 x 3 3 3 3」である。なお、公開情報 K p は、所定のサーバから取得してもよい。画像検証装置 3 0 は、抽出された 2 次検証データを検出された公開情報 K p で復号化し、ダイジェストデータ（ハッシュ値）を復元する。なお、公開情報 K p は、検証データ変換装置 2 0 B が秘密に管理している秘密

情報 K s に対応する情報であり、一般に公開されている情報である。

【 0 0 9 4 】

ステップ S 1 6 1 2 : また、画像検証装置 3 0 は、2 次検証データ付き画像ファイルのデータ部から画像データを抽出する。画像検証装置 3 0 は、抽出された画像データをハッシュ関数 H 2 によってダイジェストデータ（ハッシュ値）に変換する。なお、ハッシュ関数 H 2 は、検証データ変換装置 2 0 B のハッシュ関数 H 2 と同じハッシュ関数である。

【 0 0 9 5 】

ステップ S 1 6 1 3 : 画像検証装置 3 0 は、ステップ S 1 6 1 1 で復元されたダイジェストデータと、ステップ S 1 6 1 2 で得られたダイジェストデータとを比較し、2 次検証データ付き画像ファイル内の画像データの完全性を検証する。検証データ変換装置 2 0 B から画像検証装置 3 0 に至るまでに改変がなかった場合、2 つのダイジェストデータは一致し、画像データの完全性は確認される。また、同時に、画像検証装置 3 0 は、この画像データが画像生成装置 1 0 で生成された画像データであることを確実に確認することができる。この場合、画像検証装置 3 0 は、改変なしと判定し、その判定結果をユーザに通知する。一方、検証データ変換装置 2 0 B から画像検証装置 3 0 に至るまでに改変があった場合、2 つのダイジェストデータは一致せず、画像データの完全性は検証されない。この場合、画像検証装置 3 0 は、改変ありと判定し、その判定結果をユーザに通知する。

【 0 0 9 6 】

ステップ S 1 6 1 4 : 画像検証装置 3 0 は、2 次検証データ付き画像ファイルの改変をチェックするごとに、画像ファイルのファイル名、画像ファイルの登録日時、画像ファイルの検証日時、改変の有無などの情報を保管用メモリ 3 5 のデータベースに登録する。このような情報を保管用メモリに登録することで、検証された 2 次検証データ付き画像ファイルを管理する。

【 0 0 9 7 】

以上説明したように、第 2 の実施の形態における画像データ検証システムによれば、第 1 の実施の形態と同様に、画像生成装置 1 0 の演算リソースの性能を大

幅に向上させることなく、画像生成装置 1 0 で生成された画像データが改変されているか否かを確実に検出することができる。また、第 2 の実施の形態における画像データ検証システムによれば、第 1 の実施の形態と同様に、画像生成装置 1 0 にかかるコストを低減することができる。

## 【 0 0 9 8 】

また、第 2 の実施の形態における画像データ検証システムによれば、画像生成装置 1 0 の固有 I D に対応する共有情報 K c、秘密情報 K s 及び公開情報 K p を用いて 1 次検証データ及び 2 次検証データを検証することにより、1 次検証データ付き画像ファイル内の画像データまたは 2 次検証データ付き画像ファイル内の画像データが画像生成装置 1 0 で生成されたものであるか否かを確実に確認することができる。

## 【 0 0 9 9 】

また、第 2 の実施の形態における画像データ検証システムによれば、画像生成装置 1 0 と検証データ変換装置 2 0 B との間を 1 次検証データによって安全に保護することができ、検証データ変換装置 2 0 B と画像検証装置 3 0 との間を 2 次検証データによって安全に保護することができるので、システム全体の安全に運用することができる。

## 【 0 1 0 0 】

また、第 2 の実施の形態の画像データ検証システムによれば、共有情報 K c 及び秘密情報 K s を保持する検証データ変換装置 2 0 B をパーソナルコンピュータなどのデータ処理装置ではなく、I C カード、サーバコンピュータなどの安全性の高いデータ処理装置で実現することにより、共有情報 K c 及び秘密情報 K s の安全性を向上させることができる。

## 【 0 1 0 1 】

次に、図 1 7 のフローチャートを参照し、第 2 の実施の形態における検証データ変換装置 2 0 A の処理手順について説明する。なお、図 1 7 に示す処理手順は、プログラムメモリ 1 4 2 6 のプログラムに従って実行される。また、図 1 7 に示す処理手順は、1 次検証データ付き画像ファイルを入力するごとに実行される。

【0102】

ステップS1701：インターフェース部A1423は、画像生成装置10からの1次検証データ付き画像ファイルを受信する。

【0103】

ステップS1702：インターフェース部B1424は、1次検証データ付き画像ファイルを検証データ変換装置20Bに送信する。

【0104】

ステップS1703：検証データ変換装置20Bが1次検証データ付き画像ファイル内の完全性を検証できなかった場合、ステップS1704に進む。一方、検証データ変換装置20Bが1次検証データ付き画像ファイル内の完全性を検証できた場合、ステップS1705に進む。

【0105】

ステップS1704：この場合、インターフェース部B1424は、画像データが改変されていることを示すメッセージを受信する。制御／演算部1421は、画像データが改変されていることを示すメッセージをユーザに通知する。

【0106】

ステップS1705：この場合、インターフェース部B1424は、2次検証データ付き画像ファイルを受信する。

【0107】

ステップS1706：インターフェース部C1428は、2次検証データ付き画像ファイルをインターネットなどのネットワーク、または、メモリカードなどのリムーバブルメディア（着脱可能な記憶媒体）に出力する。

【0108】

次に、図18のフローチャートを参照し、第2の実施の形態における検証データ変換装置20Bの処理手順について説明する。なお、図18に示す処理手順は、プログラムメモリ1526の検証プログラムに従って実行される。また、図18に示す処理手順は、1次検証データ付き画像ファイルを入力するごとに実行される。

【0109】



ステップS1801：インターフェース部1524は、検証データ変換装置20Aからの1次検証データ付き画像ファイルを受信する。

【0110】

ステップS1802：制御／演算部1521は、1次検証データ付き画像ファイルのヘッダ部から1次検証データを抽出する。

【0111】

ステップS1803：また、制御／演算部1521は、1次検証データ付き画像ファイルのヘッダ部から画像生成装置10の固有IDを抽出し、そのファイルのデータ部から画像データを抽出する。制御／演算部1521は、プログラムメモリ1526内のテーブルT1を参照し、抽出された固有IDに対応する共有情報Kc及び秘密情報Ksを検出する。制御／演算部1521は、抽出された画像データと検出された共有情報Kcとからその画像データの1次検証データを生成する。

【0112】

ステップS1804：制御／演算部1521は、ステップS1802で抽出された1次検証データ（即ち、画像生成装置10の内部で生成された1次検証データ）と、ステップS1803で生成された1次検証データ（即ち、検証データ変換装置20Bの内部で生成された1次検証データ）とを比較し、1次検証データ付き画像ファイル内の画像データの完全性を検証する。2つの1次検証データの一致が検出された場合、ステップS1806に進む。一方、2つの1次検証データの一致が検出されなかった場合、ステップS1805に進む。

【0113】

ステップS1805：この場合、制御／演算部1521は、改変ありと判定し、画像データが改変されていることを示すメッセージを検証データ変換装置20Aに送信する。なお、この場合、検証データ変換装置20Bは、2次検証データの生成を禁止する。

【0114】

ステップS1806：この場合、制御／演算部1521は、1次検証データ付き画像ファイルの画像データから2次検証データ（即ち、デジタル署名）を生

成する。

【0115】

ステップS1807：制御／演算部1521は、画像ファイルのヘッダ部にある1次検証データを生成された2次検証データに置き換え、2次検証データ付き画像ファイルを生成する。生成された2次検証データ付き画像ファイルは、検証データ変換装置20Aに送信される。

【0116】

以上の処理手順により、検証データ変換装置20Bは、画像生成装置10の演算リソースの性能を大幅に向上させることなく、画像生成装置10で生成された画像データが改変されているか否かを確実に検出することができるので、画像生成装置10にかかるコストを低減することができる。また、検証データ変換装置20Bは、1次検証データ付き画像ファイルの画像データが画像生成装置10で生成されたものであるか否かを確実に確認することができる。また、1次検証データ付き画像ファイルの完全性が確認できれば、そのファイルを2次検証データ付き画像ファイル（即ち、デジタル署名付き画像ファイル）に変換することもできる。

【0117】

なお、上記の各実施の形態は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0118】

【発明の効果】

以上説明したように、本発明によれば、デジタルカメラなどの画像生成装置にかかるコストの増大を防ぎつつ、画像生成装置で撮影された画像データが改変されているか否かを確実に検出することができる。

【図面の簡単な説明】

【図1】

第 1 の実施の形態における画像生成装置 1 0 の主要な構成を説明するブロック図である。

【図 2】

第 1 の実施の形態における検証データ変換装置 2 0 の主要な構成を説明するブロック図である。

【図 3】

第 1 の実施の形態における画像検証装置 3 0 の主要な構成を説明するブロック図である。

【図 4】

第 1 の実施の形態における画像データ検証システムの処理手順を説明する図である。

【図 5】

1 次検証データの生成方法の一例を説明する図である。

【図 6】

簡易な演算の一例を説明する図である。

【図 7】

テーブル T 1 及びテーブル T 2 の一例を示す図である。

【図 8】

2 次検証データ（即ち、デジタル署名）の生成方法を説明する図である。

【図 9】

第 1 の実施の形態における画像生成装置 1 0 の処理手順を説明するフローチャートである。

【図 1 0】

第 1 の実施の形態における検証データ変換装置 2 0 の処理手順を説明するフローチャートである。

【図 1 1】

第 1 の実施の形態における画像検証装置 3 0 の処理手順を説明するフローチャートである。

【図 1 2】

第 1 の実施の形態における画像データ検証システムの構成の一例を説明する図である。

【図 1 3】

第 2 の実施の形態における画像データ検証システムの構成の一例を説明する図である。

【図 1 4】

第 2 の実施の形態における検証データ変換装置 2 0 A の主要な構成を説明するブロック図である。

【図 1 5】

第 2 の実施の形態における検証データ変換装置 2 0 B の主要な構成を説明するブロック図である。

【図 1 6】

第 2 の実施の形態における画像データ検証システムの処理手順を説明する図である。

【図 1 7】

第 2 の実施の形態における検証データ変換装置 2 0 A の処理手順を説明するフローチャートである。

【図 1 8】

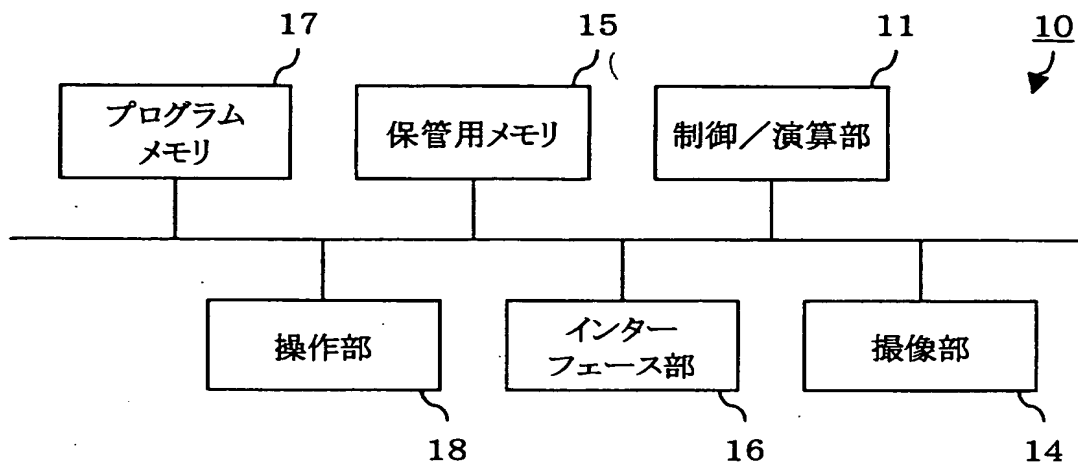
第 2 の実施の形態における検証データ変換装置 2 0 B の処理手順を説明するフローチャートである。

【符号の説明】

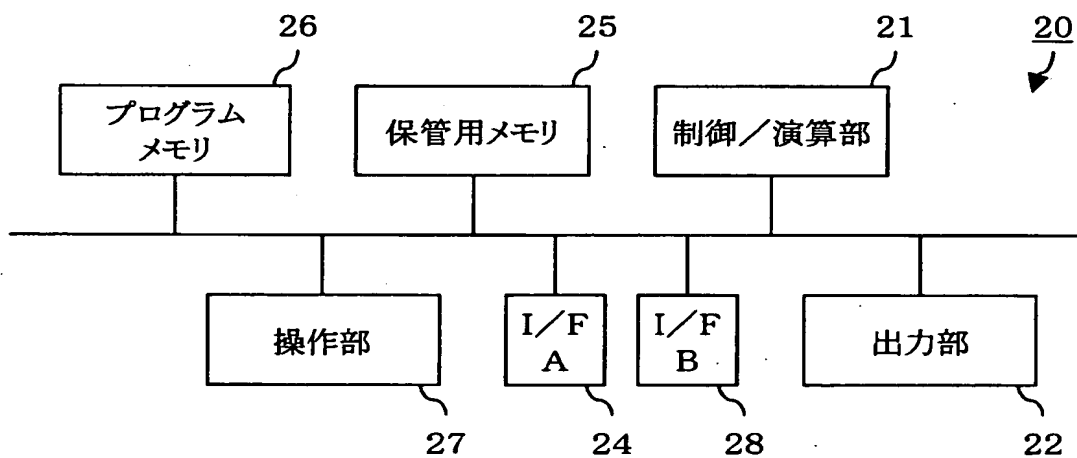
- 1 0     画像生成装置
- 2 0     検証データ変換装置
- 3 0     画像検証装置
- 2 0 A    第 1 の検証データ変換装置
- 2 0 B    第 2 の検証データ変換装置

【書類名】 図面

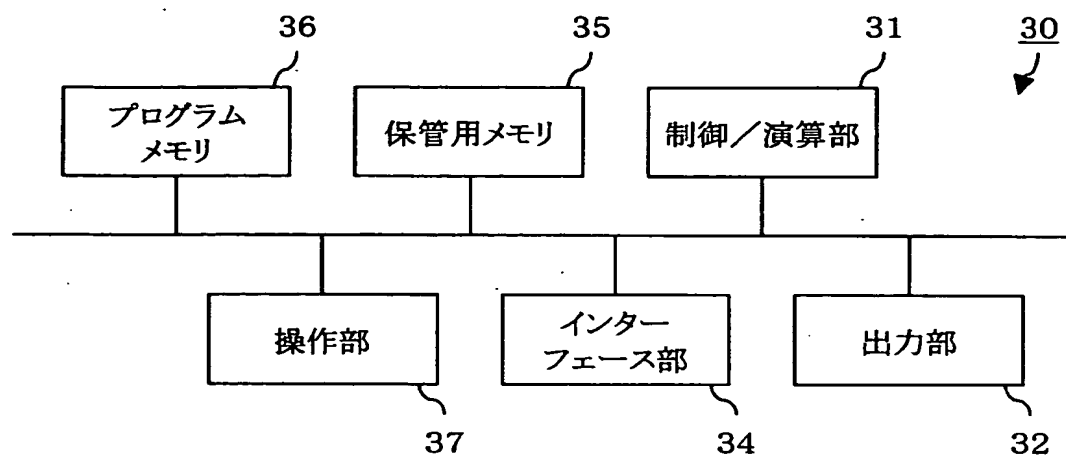
【図 1】



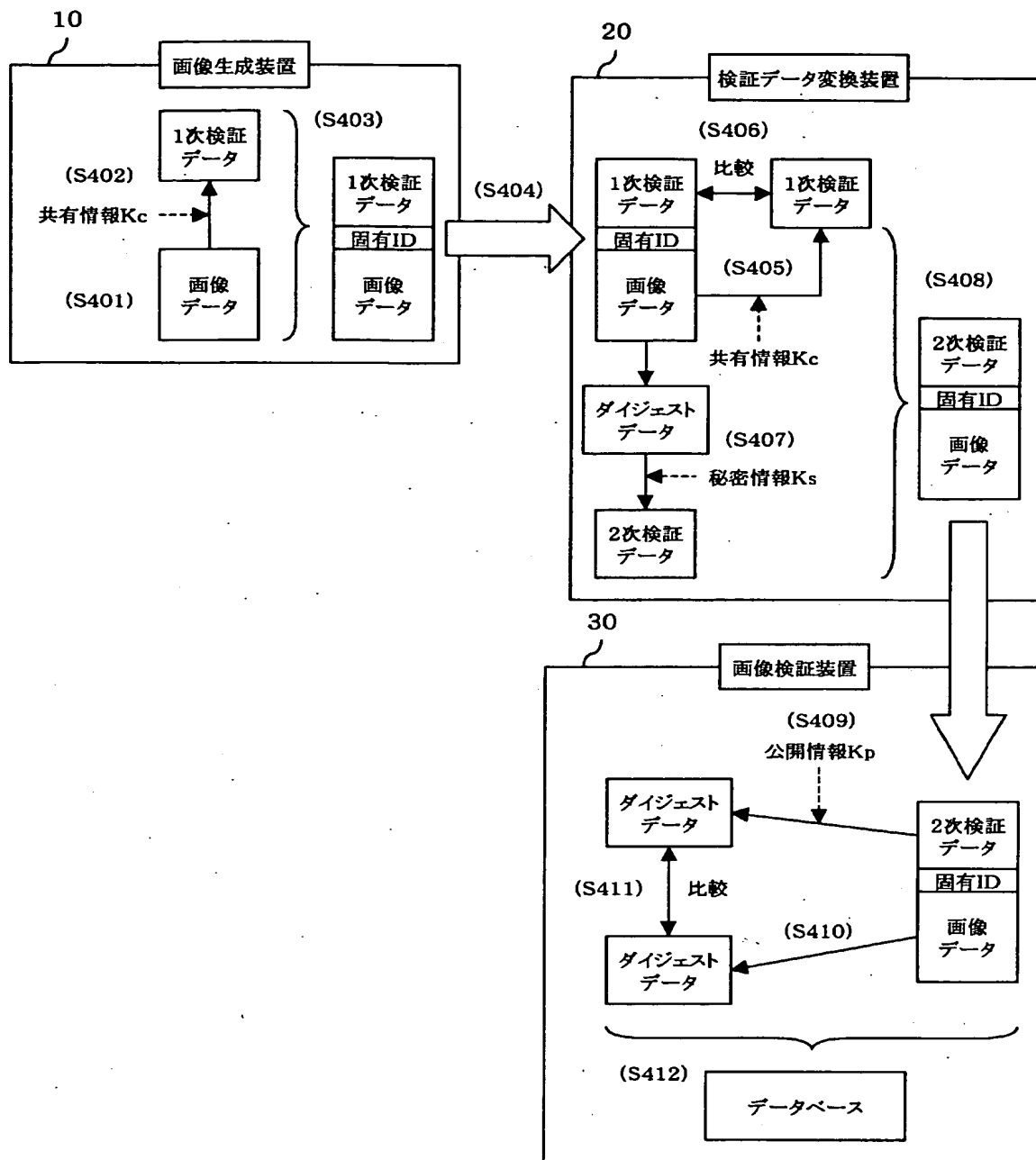
【図 2】



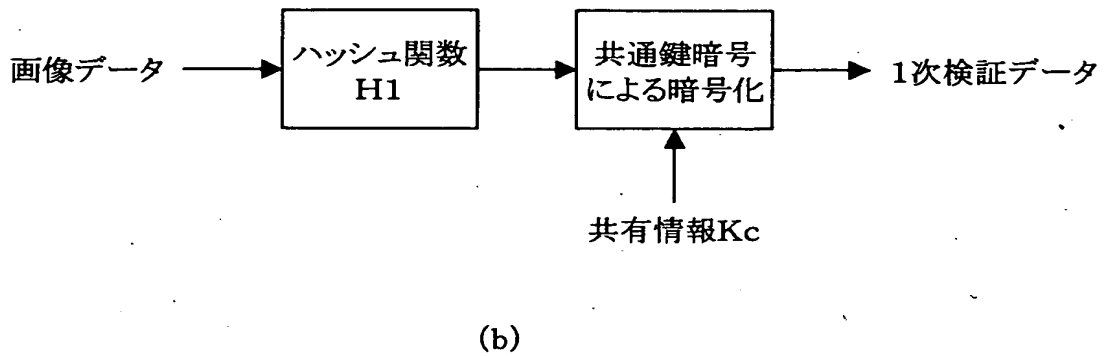
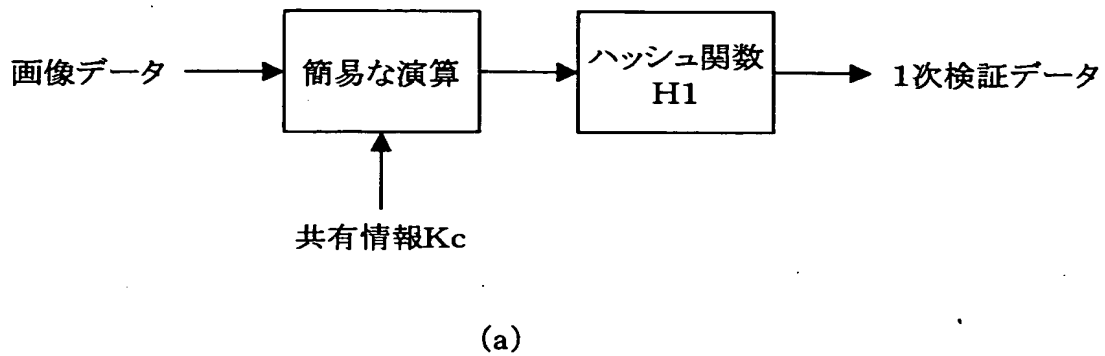
【図 3】



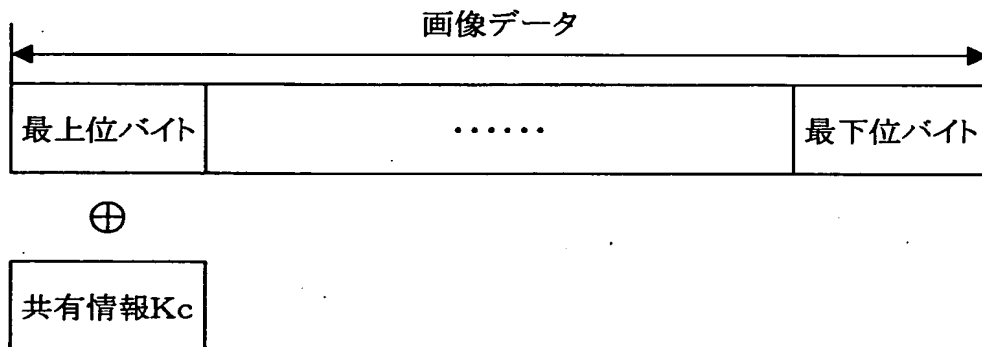
【図 4】



【図 5】



【図 6】





【図 7】

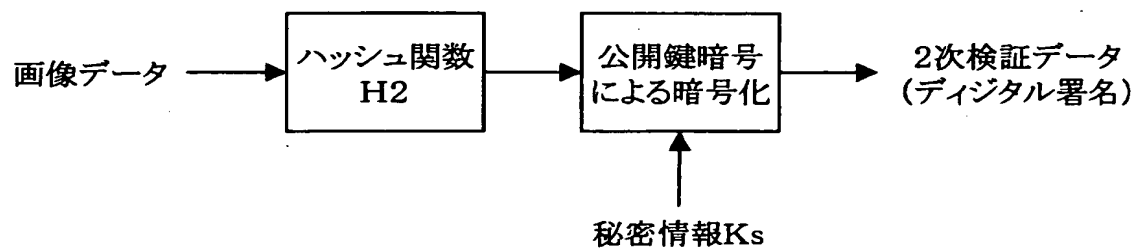
固有ID	共有情報Kc	秘密情報Ks
001	0x1111	0x2222
002	.....	.....
.....	.....	.....

(a)

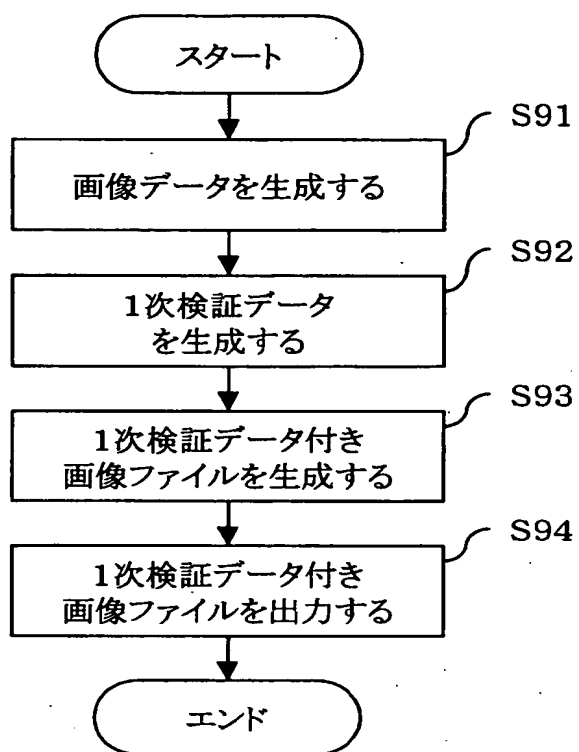
固有ID	公開情報Kp
001	0x3333
002	.....
.....	.....

(b)

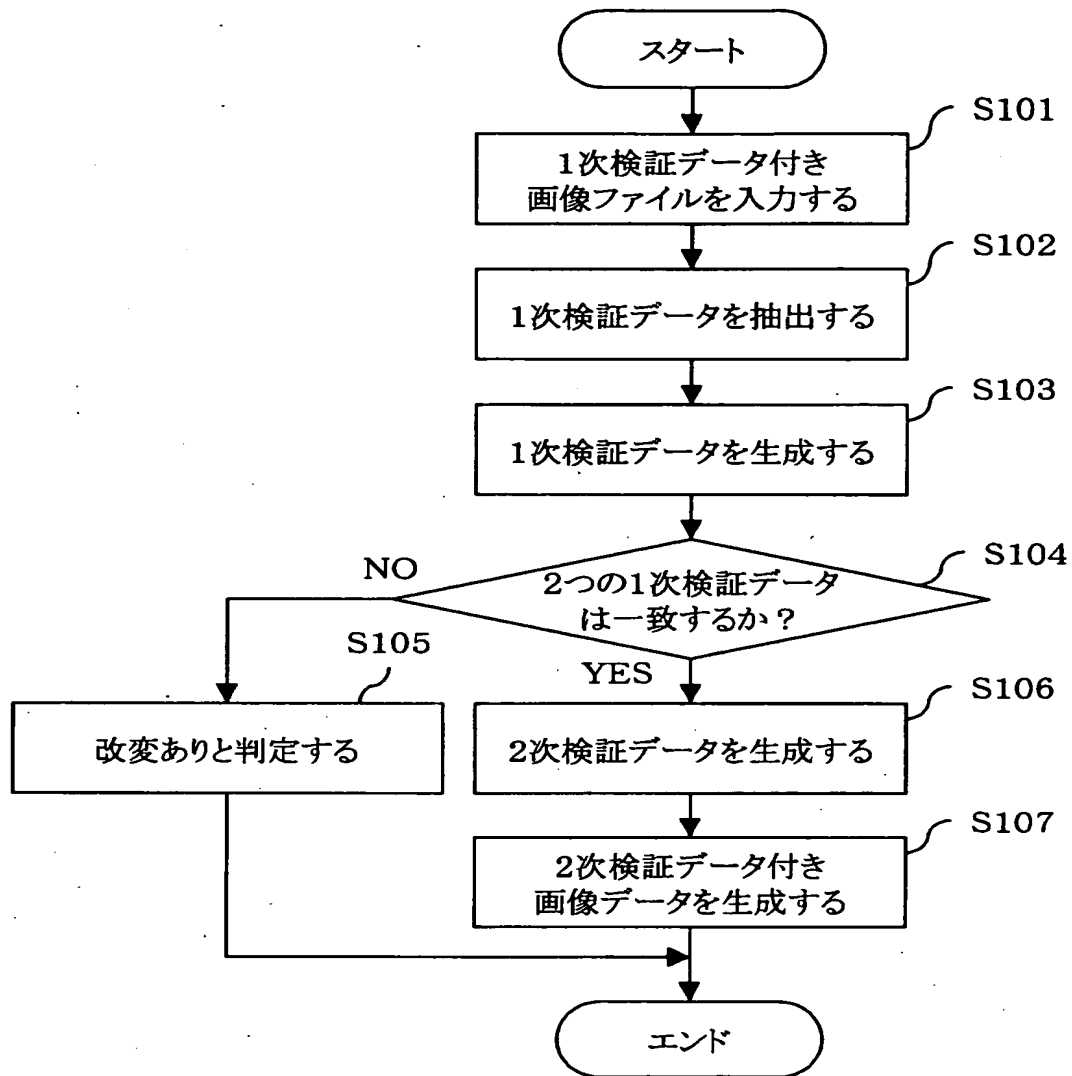
【図 8】



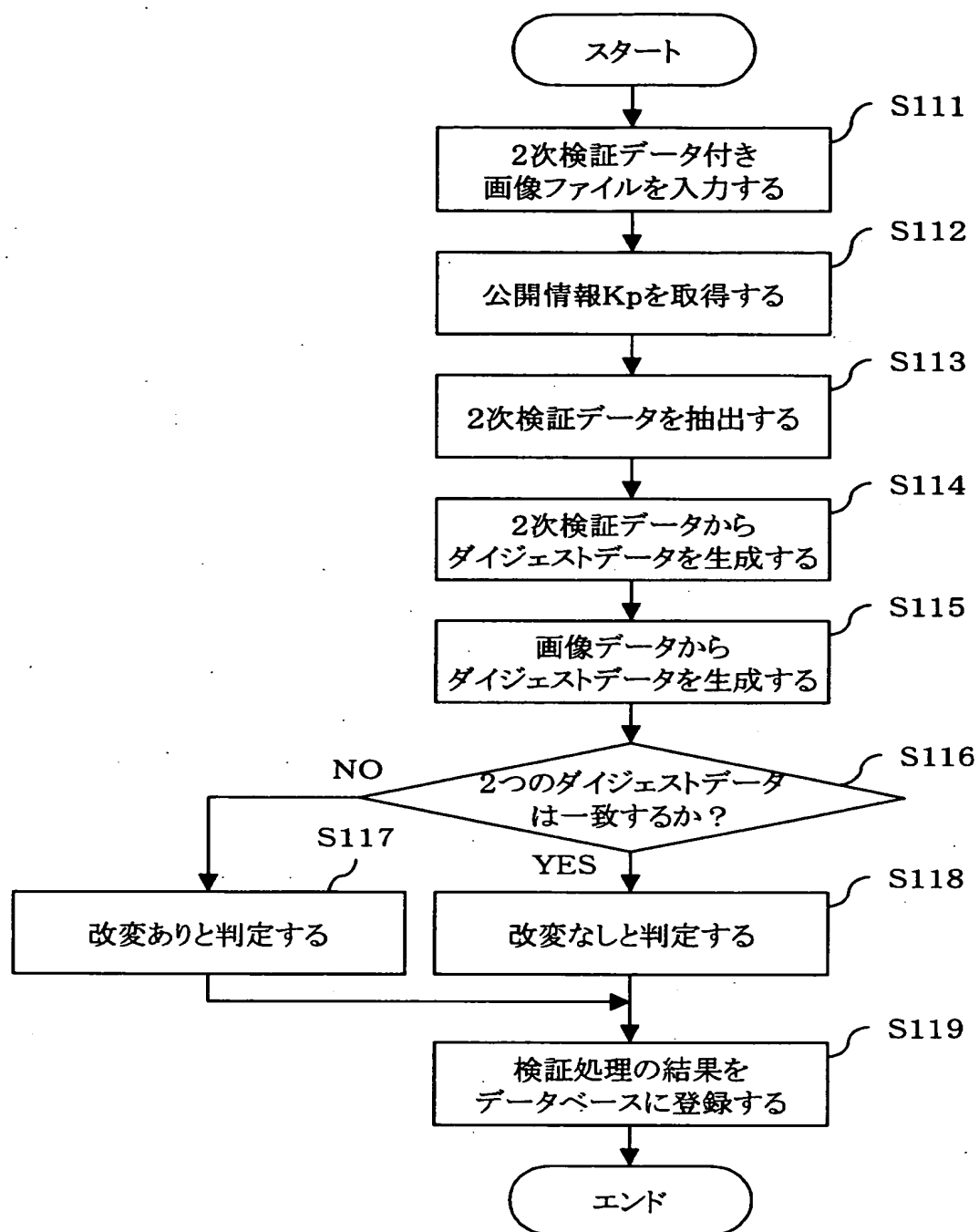
【図 9】



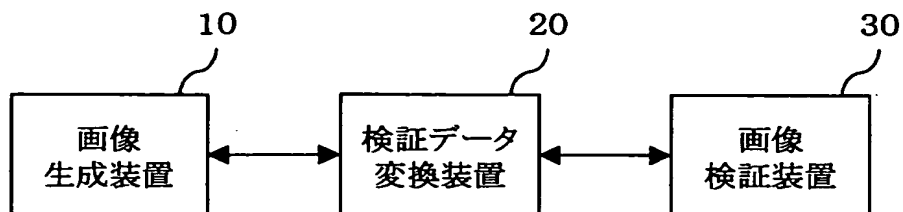
【図10】



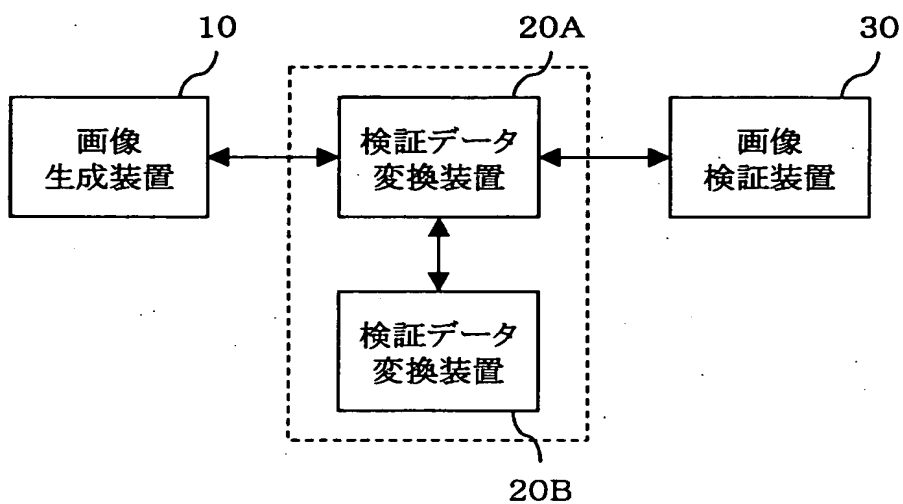
【図 11】



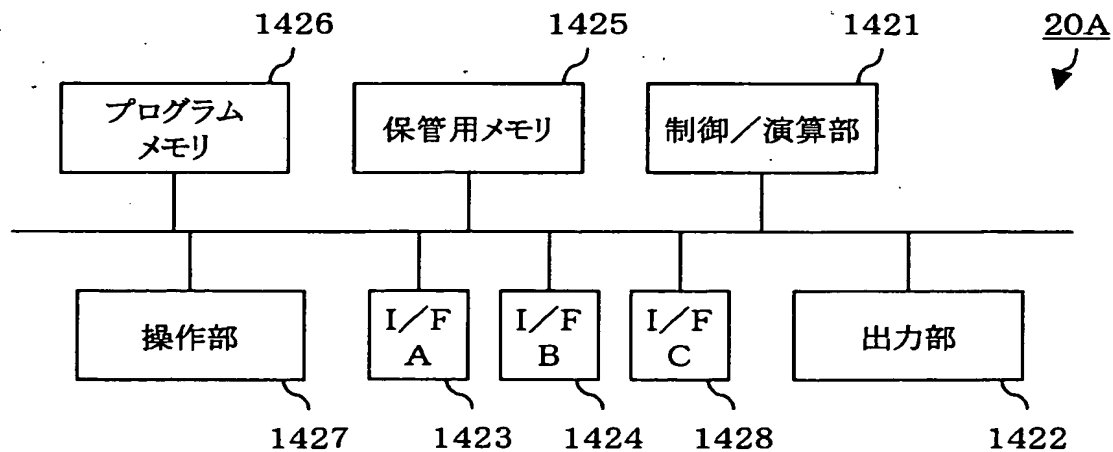
【図 12】



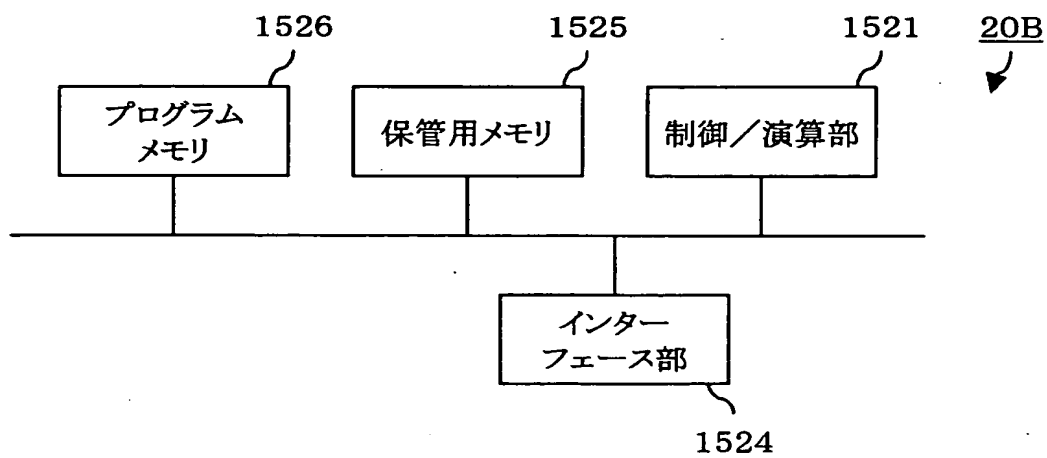
【図 13】



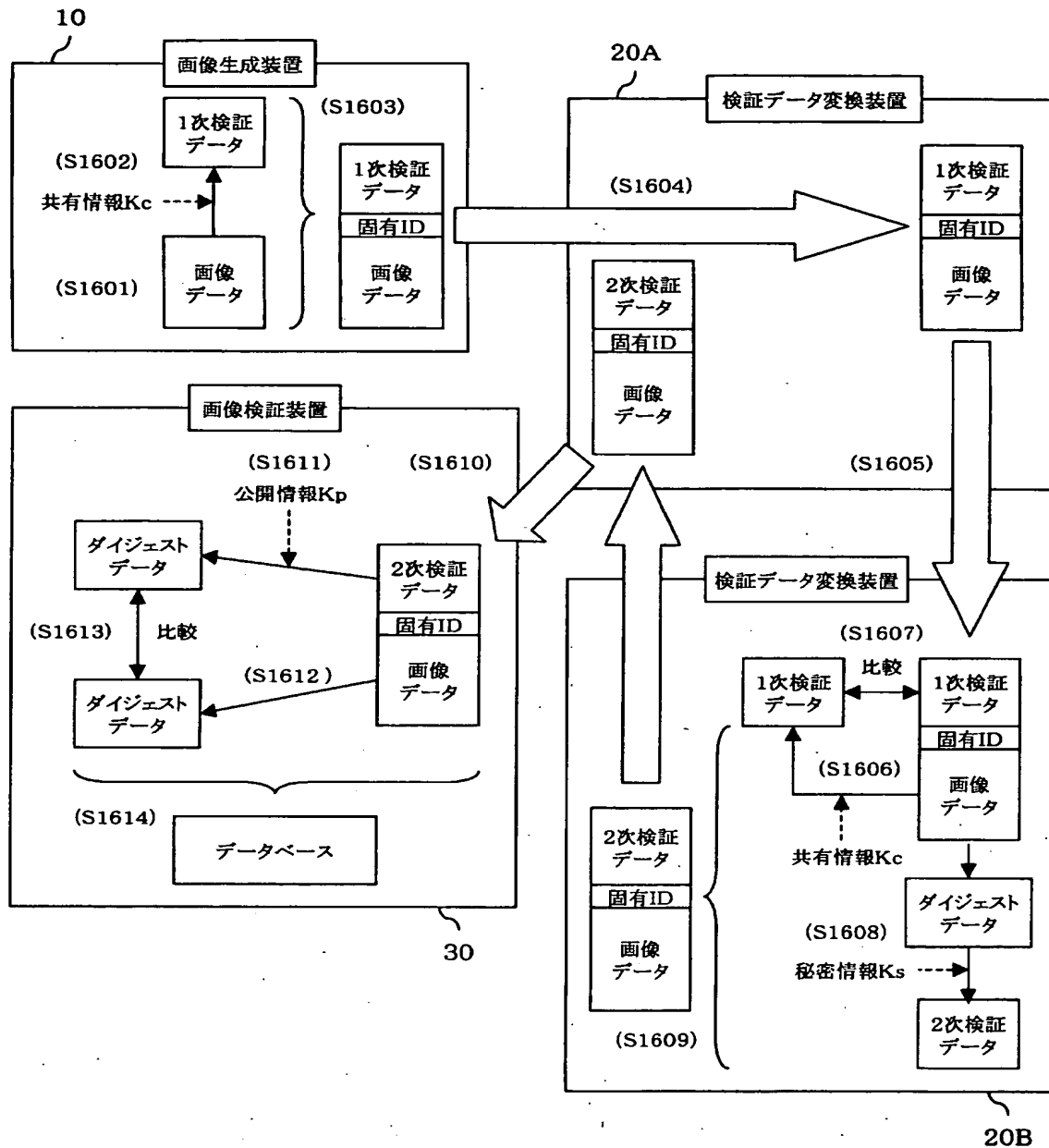
【図 14】



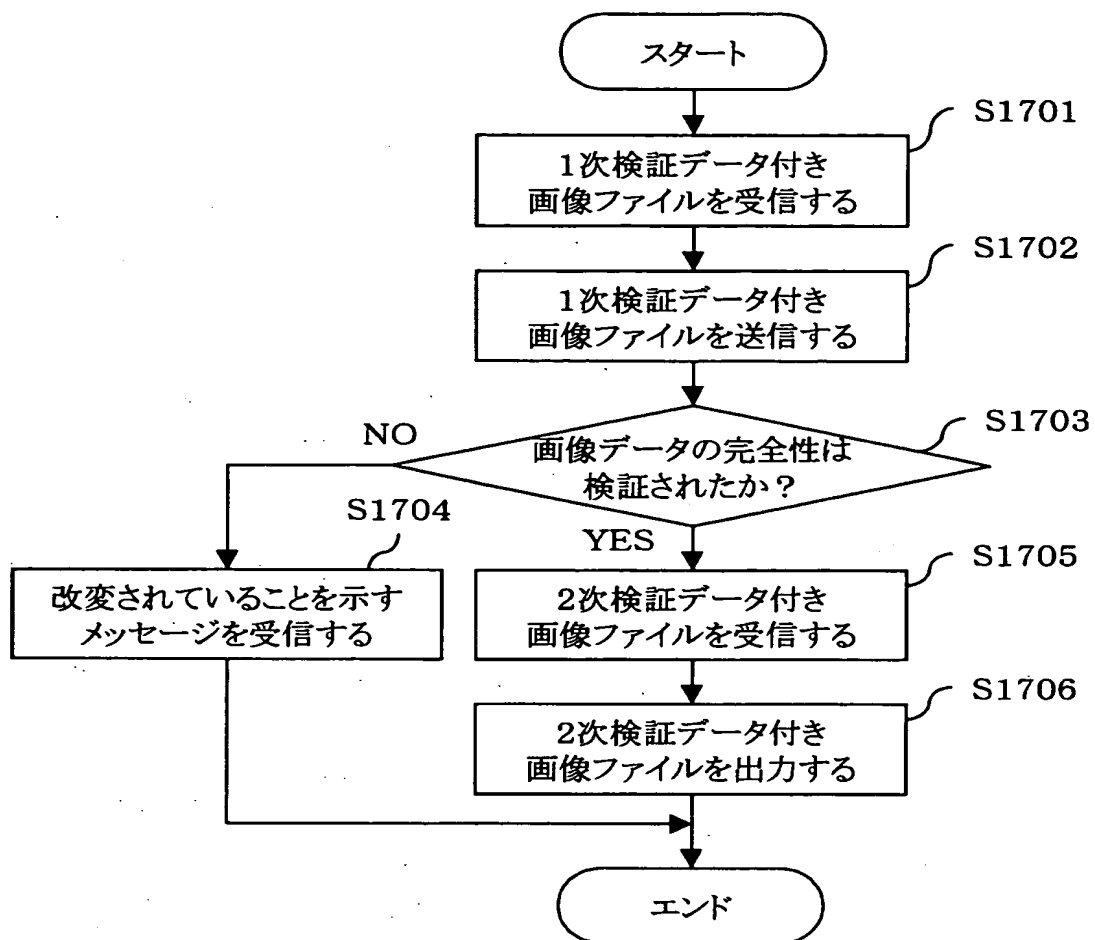
【図15】



【図 16】

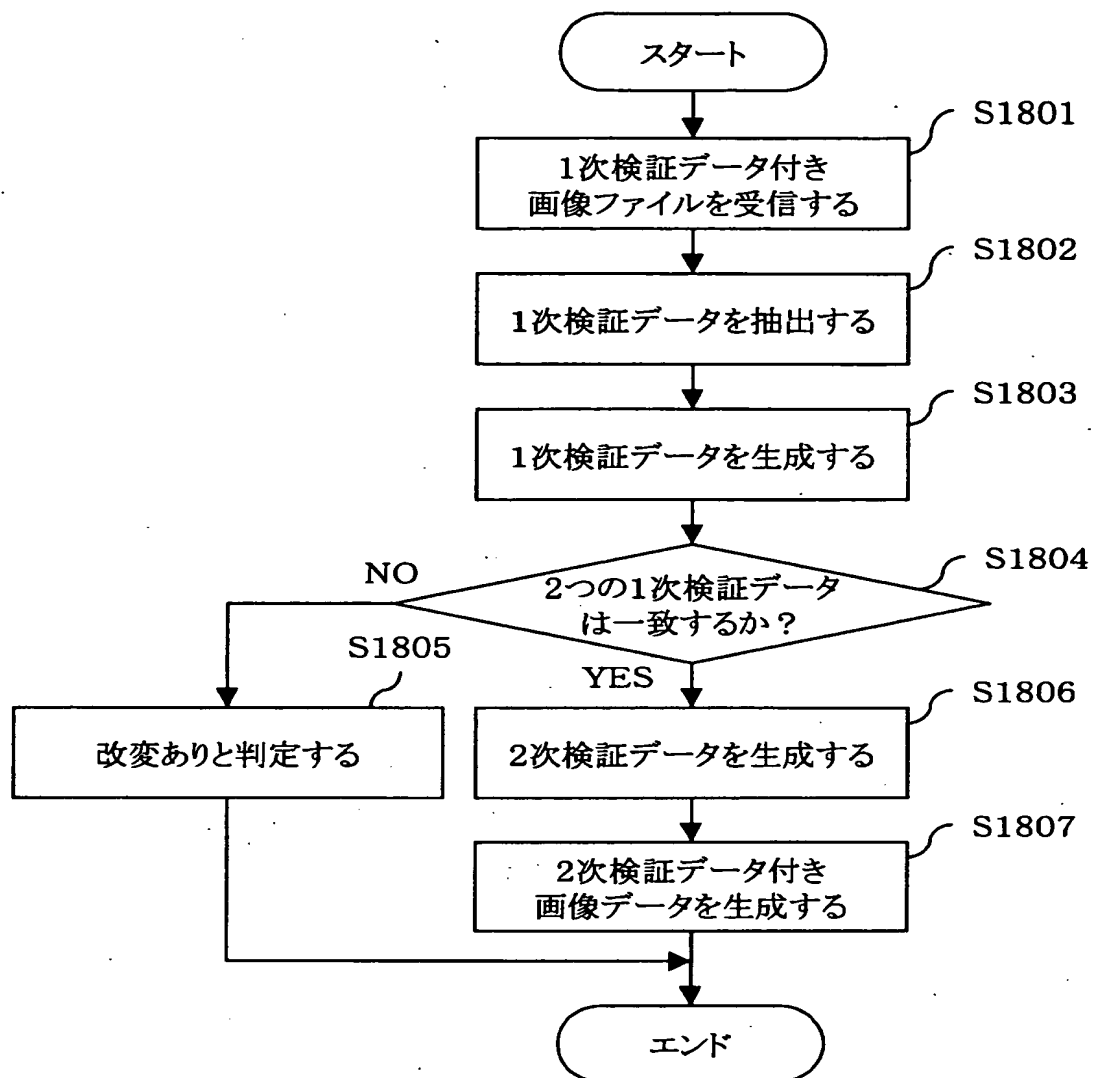


【図 17】





【図18】



【書類名】            要約書

【要約】

【課題】    デジタルカメラなどの画像生成装置にかかるコストの増大を防ぎつつ、画像生成装置で撮影された画像データが改変されているか否かを確実に検出する。

【解決手段】    画像生成装置 1 0 は、1 枚の画像データを撮影するごとに、1 次検証データ付き画像ファイルを生成する。検証データ変換装置 2 0 は、1 次検証データ付き画像ファイル内の映像データが改変されていない場合、2 次検証データ付き画像ファイル（デジタル署名付き画像ファイル）を生成する。画像検証装置 3 0 は、2 次検証データ付き画像ファイルの完全性を検証し、そのファイルが改変されているか否かを検出する。

【選択図】            図 1 2

認定・付加情報

特許出願の番号	特願2001-346689
受付番号	50101668599
書類名	特許願
担当官	第六担当上席 0095
作成日	平成13年11月15日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子3丁目30番2号
【氏名又は名称】	キャノン株式会社

【代理人】

申請人

【識別番号】	100090273
【住所又は居所】	東京都豊島区東池袋1丁目17番8号 池袋TG ホームストビル5階 國分特許事務所
【氏名又は名称】	國分 孝悦

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都大田区下丸子3丁目30番2号
氏 名	キヤノン株式会社